CALIFORNIA STATE THREAT ASSESSMENT CENTER

24-HOUR REPORT

11 OCTOBER 2017

(U) CALIFORNIA

(U) Stockton – Little Manila Center Vandalized in Possible Hate Crime
(U) The Little Manila Center was vandalized by someone who tore down window posters and painted racially charged words on the storefront. The center's staff says the vandalism is being investigated by police as a possible hate crime because of the words that were used. The center was created three years ago to celebrate the area's Filipino American history and educate residents about the contributions immigrants have made to the economy and cultural heritage of the community.
SOURCE: 10 October 2017, FOX 40

(U) NATIONAL

(U) District of Columbia – Officials Warn of Potential Hezbollah Threat to Homeland
(U) Washington – US officials previewed a new offensive against Iranian-backed Hezbollah, claiming the group aspires to conduct attacks against the US homeland. National Counterterrorism Center Director Nicholas Rasmussen said the intelligence community did see continued activity on behalf of Hezbollah here inside the homeland, citing recent arrests of alleged Hezbollah operatives in New York and Michigan. Ali Kourani and Samer el Debek were arrested in June 2017, and charged with providing material support to Hezbollah's Islamic Jihad Organization.
SOURCE: 11 October 2017, CNN

(U) Georgia – Equifax Hack Disclosed Driver's License Data for More Than 10 Million Americans
(U) Atlanta – Driver's license data for around 10.9 million Americans were compromised during the recent breach of Equifax Inc.'s systems, according to sources familiar with the matter. The license information was accessed by hackers who also took vital personal information, including Social Security numbers, of potentially 145.5 million Americans. Separately, Equifax said yesterday that a file containing 15.2 million UK consumer records was attacked during the company's hack. Equifax announced the breach, which also affected consumers in Canada, on 7 September. At that time, the company said that "in some instances" US driver's license numbers were accessed, but didn't publicly say how many.
SOURCE: 10 October 2017, FOX Business

(U) New York – Hack Hit Server Containing Emails from Across US Government
(U) New York City – The hack into the accounting firm Deloitte compromised a server that contained the emails of an estimated 350 clients, including four US government departments, the United Nations, and some of the world's biggest multinationals. The incident is potentially more widespread than Deloitte had been prepared to acknowledge, with the company not fully sure what was taken. Deloitte previously said it believed the hack had only impacted six clients, and that it was confident it knew where the hackers had been. The US government agencies and companies believed to have been affected are the US Departments of State, Energy, Homeland Security, and Defense; the US Postal Service; the National Institutes of Health; and "Fannie Mae" and "Freddie Mac", the housing giants that fund and guarantee mortgages in the US.
SOURCE: 10 October 2017, The Guardian

(U) Washington – Website Allowed Hackers to Access Account Data
(U) Bellevue – Last week, a bug was removed from a T-Mobile website that allowed hackers access to personal data such as an email address, a customer's account number, and the phone's international mobile subscriber identity (IMSI), a standardized unique number that identifies subscribers. The flaw allowed malicious hackers who knew—or guessed—customer phone number to obtain data that could have been used for social engineering attacks, or perhaps even to hijack victim's numbers.
SOURCE: 10 October 2017, Mother Board

Form # 1168-442e-b407-de1a8c242c14

(U) INTERNATIONAL

(U) Australia – Cybersecurity Report Shows Gaps in Private Companies' Defenses
(U) Melbourne – The Australian government presented its annual cybersecurity report yesterday, revealing that one of its national security contractors had suffered a breach in which a significant amount of data was lost last year. Included in the report was a case study that said the government's cybersecurity team discovered that an attacker had compromised the network of a small company with contracting links to national security projects. The report also added that the attacker was on the network for an extended period. The revelation of the security contractor's breach, and the lack of detail surrounding it, comes at a time of increased concern over the government's ability to protect citizens' personal information—especially when accounting for third parties that have access to sensitive data.
SOURCE: 10 October 2017, New York Times

(U) Belgium – New Suspect Charged In 2016 Suicide Attacks
(U) Brussels – Belgian authorities have arrested and charged a man with terrorism offenses over the March 2016 suicide bombings in Brussels, the latest in the ongoing case, prosecutors said today. The 39-year-old man named as Brahim T., a Belgian national, was arrested on a warrant from an investigating judge and is due to appear in court for a pre-trial hearing in the next few days. Prosecutors gave no details about his ties to the suicide bombers who killed a total of 32 people at Brussels International Airport and a metro station in the Belgian capital. Nine people have previously been charged over the attacks.
SOURCE: 11 October 2017, Agence France-Presse

(U) PREPARED BY THE CALIFORNIA STATE THREAT ASSESSMENT CENTER.

(U) FOR QUESTIONS OR CONCERNS, PLEASE EMAIL STAC@CALOES.CA.GOV, OR CALL 916-636-2900.

This document contains excerpts of suspicious activities and incidents of interest to the STAC as obtained from open and unclassified sources.